Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020
7-10 January 2020, Maui, Hawaii. DOI:10.24251/HICSS.2020.230

Toward a holistic model of deception: Subject matter expert validation

Iain D. Reid
University of Portsmouth
Iain.reid@port.ac.uk

Robert Black
Cranfield University
r.black@cranfield.ac.uk

Abstract

Security challenges require greater insight and flexibility into the way deception can be identified and responded to. Deception research in interactions has identified behaviors indicative of truth-telling and deceit. Deception in military environments has focused on planning deception, where approaches have been developed to deceive others, but neglecting counter-deception perspectives. To address these challenges a holistic approach to deception is advocated. A literature review of deception was conducted followed by validation interviews with Subject Matter Experts (SMEs). Explanatory thematic analysis of interviews conducted with SMEs (n=19) led to the development of meta-themes related to the 'deceiver', their 'intent; 'strategies and tactics' of deception, 'interpretation' by the target and 'target' decision-making strengths and vulnerabilities. This led to the development of the Holistic Model of Deception (HMD), an approach where strategies reflect context. The implications of this approach are considered alongside the limitations and future directions required to validate the HMD.

1. Introduction

The current paper defines deception as "*a deliberate attempt, without forewarning, to create in another a belief which the communicator considers to be untrue, with the aim of influencing the receivers' mindset (manner of thinking structured by their attitudes, personality and culture) and/or behavior*". This definition is applicable across interpersonal and mediated environments, whether the act is verbal, non-verbal or physical, and emphasizes that the aim of deception is to change the receiver's behavior through implanting or enabling the target to generate a false belief, ensuring applicability to online and military environments. This definition of deception is a refinement of that of [48] who primarily focus on deception, but we incorporate cognition and behavior.

[41] propose a theoretical holistic model of deception incorporating traditional and differential recall enhancement (DRE) [9] approaches to credibility assessment alongside multiple-cue and multiple-sourcing approaches. A further consideration of the effects of culture, personality and individual differences, motive and mindset are discussed. Deception cannot be avoided; indeed deception will occur whenever and wherever adversaries are seeking an advantage [3, 51]. Deception should be anticipated as occurring across a range of environments and greater understanding of how deception emerges and is responded to in complex environments is required. In this article, holistic, online, and military approaches to deception are reviewed, before the validation of a holistic approach to deception through interviews with Subject Matter Experts (SMEs) including researchers and practitioners working in diverse fields of deception.

2. Literature Review

2.1. Holistic Approaches

Holistic approaches to deception combine verbal and non-verbal cues [39, 45], and knowledge of background, personality, cognition, culture and environmental factors [31] to increase accuracy in detecting deception. As credibility assessment may be adversely affected in cognitively challenging and group decision-making environments [31] there is a need to implement a bespoke holistic approach to deception detection which incorporates an understanding of decision-making to counter potential vulnerabilities.

[4] counter-deception approach examines 'intelligence functions' including deception cues, deception detection and exposure, adversary discovery and penetration alongside 'operational functions' incorporating mitigation and exploitation of adversary deception. These functions are argued to be highly interdependent and present deception as a continuum of functions rather than individual elements [4].

URI: https://hdl.handle.net/10125/63969
978-0-9981331-3-3

Human reasoning and self-assessment of own biases, beliefs and methods of intelligence gathering, and intelligence-gathering channels will identify potential vulnerabilities potentially mitigating the effects of deception [4]. Multiple channels of information enable a greater range of HUMINT with which to assess credibility [4]. Threat and situation assessments are required to understand the influences and circumstances in which deception may occur [4] and such approaches parallel more recent psychological approaches to understanding high-stakes future intent [19].

To increase accuracy in deception detection in complex operating environments, [41] propose using a combination of verbal, nonverbal and paralinguistic cues to deception alongside a consideration of personality and individual differences, motive, mindset and consideration of decision-making. Cues are argued to reflect context and may not be applicable across all instances of deception [2]. The multiple cue approach incorporates consideration of low-stakes [47], high stakes [39] and rapid judgement [47] environments and hence such evidence supports a holistic, tailored approach. [41] propose multiple-sourcing alongside multiple-cues whereby different sources of information can be examined for consistency increasing available knowledge for credibility judgements. The incorporation of the CHAMELEON Approach [18] (which focuses on targeting interviewing strategies according to context) into a holistic approach to deception by [41] highlights that individual's behavior and the strategies they use to present themselves change across contexts. The impact of culture, religiosity and belief system on deception is incorporated into a holistic approach to deception [41].

2.2. Online Approaches

Deception detection in online contexts may be challenging [17] and requires consideration of linguistic patterns [22], the use of 'warrants' (connections between online and real-world identities) to confirm a sender's identity [50], 'digital footprints' and 'scent trails' to uncover malign intent [42], and adaptations of computer-mediated investigative interviewing approaches [9, 15, 29]. Regarding the influence of third party opinions, [36] examined the linguistic features of online reviews to identify truthful and deceptive opinions and found that truthful reviews contained more concrete and sensorial language and were more accurate about spatial information, whilst deceivers focused upon elements not directly related to the subject they were reviewing and, in contrast to previous research [35], used more positive language. This has implications for understanding the content of opinions and speeches posted in online environments, especially in higher stake situations where such views can sway public belief and behavior, for example, reviews may have a large impact on auction fraud, whilst deceptive opinions may affect support for on-going regional conflicts.

In the online environment the ability to alter identity benefits those who engage in malign acts, regardless of the deceptive nature of the behavior. The malign intent of a child sexual offender purporting to be a child while grooming a victim, or a sadistic stalker who presents in a chameleon manner provides a more concerning presentation of behavior and intent. This becomes further problematic when offending behavior is online and offline and individuals use aliases to reduce the likelihood of detection. The use of 'warrants' enable links to be examined between an individual's real-world and online identities [50] and deception may occur more routinely in online chat environments that enable greater anonymity, and less often in the use of email where warrants are visible but can be modified to mislead. Although examining 'warrants' may be a useful strategy for assessing credibility in low-stakes online interactions, in high-stake interactions the levels of sophistication employed by groups and individuals to cover their identities and tracks are greater, as is the motivation, level of resources and ability to manipulate.

Uncovering hidden deception and malign intent across interpersonal and online environments can include the identification of 'digital footprints', 'digital exhaust' or 'scent trails' that can be coupled with collateral evidence such as surveillance footage [14, 42]. Although rarely the focus of traditional deception approaches, examining patterns of behavior, including email communications, online statements and online searches of information about potential targets [14] may enable the identification of concealed actions. In a holistic approach to deception, a proactive stance is required where potential adversaries are being monitored to ensure that information is collated and assessed for deceit. Furthermore, there is potential for collected evidence to be later used in investigative interviews with which to challenge suspect's narratives.

2.3. Military Approaches

Approaches to detecting deception in the military environment have focused on analysis of competing hypotheses (ACH) [26, 43], the Busby-Whaley Ombudsmen technique, and a more holistic approach to counter-deception advocated by [4]. ACH consists of a series of steps firstly involving the identification of possible hypotheses, secondly listing evidence and

assumptions for and against each hypothesis, thirdly drawing tentative conclusions about the likelihood of each hypothesis, analysis of the sensitivity of the conclusion to significant evidence, and lastly the identification of future observations that would confirm or eliminate the hypotheses [43]. To counter confirmation biases and aid decision-making [26] recommends that there should be an increased emphasis on seeking refutations for hypotheses rather than confirmations. ACH is a promising method of supporting decision-making processes involved in detecting deception, as there is the potential to incorporate a broader range of factors including human behavior, motivation, intent and mindset alongside evidence developed from HUMINT.

[52] propose a theory of counter-deception based upon approaches applicable to multiple contexts. They identified nine categories of cues (pattern, players, intention, payoff, place, time, strength, style and channel) which are elements that the deceiver may conceal or reveal during deception [52]. The major principle of this approach is the 'plus-minus rule' where cues may indicate deception by their presence or absence and the 'congruity-incongruity rule' is suggested where deception may prove challenging to identify and requires further investigation [52]. Techniques include: 'Locard's exchange principle' – where a deceiver may leave evidence at the scene and take some away; 'verification' – of the deception; 'the law of multiple sensors' – examination of multiple channels for deceit; 'passive and active detection' – the examination of current evidence and the search for further evidence; 'pre-detection' – where understanding an adversary's deception modus operandi, goals and capabilities may uncover potential deception; 'penetration and counterespionage' – uncovering an adversary's plans through espionage and neutralizing adversary operatives to protect target infrastructure; 'the prepared mind and intuition' – where preparation for deception and the intuition to detect it enables counter-deception; and 'indirect thinking and the third option' – the ability to detect potential adversary options for deception is required for counter-deception. [52] final element is the 'Ombudsman Method' where irrelevances, discrepancies and misdirection are examined alongside indirect thinking and intuition [4]. This approach to deception detection appears promising where elements may be adopted towards a holistic approach particularly regarding using multiple sources of HUMINT, and active deception detection alongside alternative ways of considering threats.

A bespoke, tailored approach to deception creates individual assessments of veracity across situations and ultimately meets the requirements of practitioners. The current research seeks to refine and expand the theoretical holistic approach to deception developed by [41] through interviews with SMEs in deception. In military environments there are limited opportunities for practitioners to develop skills necessary in countering adversary deception and in deceiving others; to overcome this limitation [52] propose an incorporation of knowledge from a wide range of areas to identify techniques used to uncover deception. Through adopting an in vivo approach to research and incorporating a wide range of SME knowledge a more robust approach to deception detection can be developed.

3. Data Collection Method

3.1. Participants

An opportunistic, snowballing sample enabled the recruitment of 19 SMEs in deception. The sample comprised 14 (74%) males and 5 (26%) females, of which, 15 (79%) were European and 4 (21%) were North American. The average length of expertise within the SME cohort was 17.6 years (SD = 11.46) ranging from 5 to 42 years' experience. Participants had expertise in both singular and multiple areas of deception. Overall participants had expertise in the following areas: interpersonal deception (N = 12), online deception (N = 6), military deception (N = 5), influence (N = 2) and personality (N = 4).

3.2. Materials

Interview schedules were developed for the interpersonal, online and military domains of deception and credibility assessment. Interview questions were designed to elicit SMEs knowledge of deception. Interview questions were focused around the environments in which deception occurs, strategies that deceivers use to convince others of their credibility, the potential impact of personality on deception, current strategies of deception detection and potential ways to improve them, parallels between the domains of deception, and the identification of potential future threats. A digital Dictaphone was used to record interviews which were stored securely on an Ironkey to ensure security and transcribed verbatim. Hardcopies were additionally stored in a secure environment.

3.3. Procedure

Participants were identified as SMEs if they had academic or practitioner experience in deception. Participants were initially approached via email or

face-to-face contact and followed up by an email inviting them to participate in research seeking to develop a holistic model of deception. Of the 41 individuals who were asked to participate in the research, 19 agreed. A general interview schedule was included as an email attachment to enable participants to examine the questions being asked of them, although interviews were further tailored to SMEs areas of expertise. Due to the nature of some of the work undertaken by SMEs approached, two different interview schedules were made available to participants, one interview schedule including interpersonal and online topics was provided to participants without appropriate security clearances and another interview schedule including interpersonal, online and military topics was provided to those participants with appropriate security clearances. Once participants had read through the information sheet and agreed to participate in the research, they were informed that their data would be anonymized and stored in a secure location, that they had a two-week window to withdraw their data if they so choose. Participants were then interviewed at a location of their choice and convenience. Following the interviews participants were debriefed about the aims of the research and thanked for their input. Ethical approval for this research was granted by the Ethics Committee of the School of Psychology of the University of Lincoln.

3.4. Data Analysis

Responses were transcribed verbatim and treated from a critical realist perspective [6] where responses were considered as reflecting reality whilst acknowledging they were generated as part of the interview procedure. An explanatory thematic analysis [21] at the semantic level was conducted according to the conventions outlined by [6]. First, familiarization with the data set occurred through transcription, and initial idea generation. Second, initial coding of relevant data was conducted. All codes were discussed with the research team and revised according to their input. Third, codes were gathered together into themes. Fourth, themes were reviewed against coded extracts and the entire data set. Fifth, clear naming and defining of themes was conducted, followed by the sixth stage, construction of the report. The explanatory thematic analysis resulted in the generation of 5 meta-themes across the process of deception.

4. Analysis and Discussion

4.1. Key Findings

Analysis of SMEs responses led to the identification of 5 meta-themes related to the process of deception and its detection, including the meta-themes of 'Deceiver', 'Intent', 'Deception Tactics', 'Interpretation' and 'Target' (See Figure 1). These themes put forward a comprehensive view of deception from the deceiver actions, intentions, deception components, information interpretation, and target elements, including vulnerabilities.

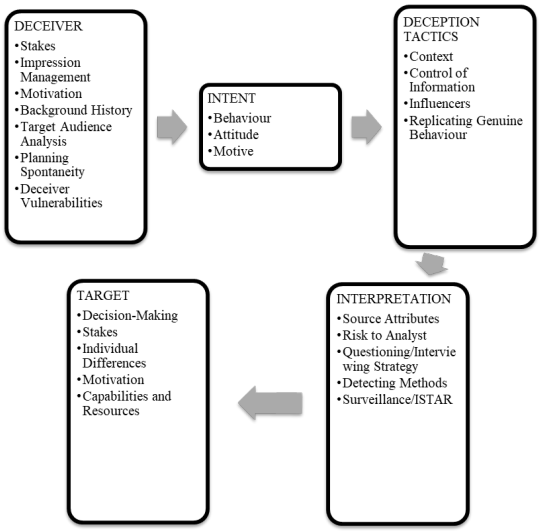

Figure 1: Holistic Model of Deception

The Holistic Model of Deception (HMD) integrates interpersonal deception theory (IDT) [7] and features-based models of credibility [12, 27, 30, 33, 53]. The HMD proposes that the context will affect the form of interaction used, how the deceiver will behave in that interaction and the techniques that will be deployed to detect deception. Multiple interpretation techniques, where applicable, can be used simultaneously to detect deception building upon recommendations by [39] that multiple-cues to deception are used, multiple sources will also be used alongside an awareness of personality, individual differences, mindset and background history.

[41] proposed a model of deception, which focused upon the elements of deception and provided a framework of individual differences that will affect the deceiver and the target. The HMD has built upon this model through the examination of diverse deception elements and individual differences across the deceiver, their intent, their strategy, ways of interpreting information and the target. Understanding the process of deception requires an iterative process where the HMD will be revised in future to reflect new

developments in understanding of the deceiver, their intent, deception tactics, strategies of interpreting information and assessing credibility and understandings of the target's decision-making processes. The key findings of each theme are outlined below.

4.2. Deceiver

The first meta-theme identified from the dataset was 'Deceiver', this meta-theme incorporates sub-themes related to 'Stakes', 'Impression Management', 'Motivation', 'Background History', 'Deceiver Vulnerabilities', 'Target Audience Analysis', and 'Planning Spontaneity'. The themes examine factors influencing how the deceiver makes decisions regarding deception and their potential ability to appear credible whilst deceiving. High-stakes situations may prove more challenging to appear credible [46] than in low-stakes where deceit may have little consequence. High-stakes situations are argued to increase anxiety and cognitive load in some deceivers leading to the identification of cues to deceit [39]. In strategic environments deceivers may place more emphasis upon carefully designing deception plans to avoid highlighting cues to deceit.

'Impression Management' examines the strategies, which the deceiver uses to appear credible to others across different environments. Previous research has focused upon how people manage their statements [24] and body language [28] and [18] proposed a series of distinct personality-based behaviors which are used to influence and persuade others of their credibility. Online approaches to impression management have focused upon the design features of websites and how people present themselves [47]. Incorporating 'Impression Management' into a holistic model of deception will enable practitioners assessing veracity in security and intelligence settings to understand the ways in which people and information are constructed to appear credible according to context.

The 'Motivation' of the deceiver will have an impact on how they deceive others and the deceiver's motivation is closely linked to the 'Stakes' of the situation. In interpersonal deception, motivation has been found to impair deceiver's ability to deceive others [11]. However, this may not occur in all circumstances, as individual differences will influence cognitive abilities during interviewing. In the online environment 'Motivation' has an enhancing effect on deception [23]. This would suggest that motivated deceivers would seek to influence others through online communication channels where there is an increased chance of success. 'Motivation' will affect how far the deceiver is willing to plan their deception and this may vary according to goals and the context in which to achieve these goals.

'Background History' of the deceiver, including their personality, individual differences, their culture and language, and previous interactions with the target is required in a holistic model of deception as this will affect their interactions with the target and the strategies, they use to deceive them. This includes their mindset at the commencement of the deceit. Knowledge of an adversary's background history, culture, individual differences and mindset factors [31, 40] can increase our ability to accurately detect deception; the current research further incorporates knowledge of personality and its impact on deception, alongside knowledge of previous interactions with the adversary and what the outcomes were. An individual's culture and language will present additional challenges to the target as this affects how they will view information presented by a deceiver from another culture [16]. In multicultural operating environments an awareness of the impact of culture is required to avoid decision-making errors. [18] highlight that individual's background histories and previous experiences will affect how they will behave in future interactions, and these same principles can be applied to the holistic model of deception.

'Deceiver Vulnerabilities' will affect how the deceiver will appear credible to others and open up pathways of detecting deception. The impact of emotional arousal, cognitive load and decision-making biases will adversely affect the deceiver's ability to appear credible. The lack of emotions in some contexts adversely affects deceivers whereby they fail to present emotions that are expected, and that truth-tellers often experience [45]. Cognitive load adversely affects deceivers as it reduces capacity to present a credible argument [48]. These vulnerabilities in the deceiver can be exploited during the 'Interpretation' phase of the model and cues to deceit identified.

When seeking to deceive others, 'Target Audience Analysis' is often conducted which will enable a deceiver to develop an enhanced understanding of the audience and identify key individuals and organizations to target. A deceiver's ability to successfully conduct 'Target Audience Analysis' affects their ability to influence the target through whatever strategy has been selected for influence, and deceiver skill will play a role in how effective this is [32]. Although 'Target Audience Analysis' as a concept has emerged from strategic environments the idea of deceivers carefully selecting and exploiting the target can be seen in both interpersonal and online environments. The deceiver may carefully develop or spontaneously perform an act of deception to a specific

target and 'Planning Spontaneity' emerged as a sub-theme in the data.

Different levels of preparation are required for different situations where there is a need to appear credible. The level of planning that the deceiver puts into their deception will affect their ability to convince others that they are credible [44]. The current research highlights that poor planning can be identified or that deceiver's strategies may subsequently collapse from challenges to their narrative. However, in long-term strategic deception, planning will play far great emphasis highlighting adversaries should be monitored and assessed for threat.

4.3. Intent

A need to understand the 'Intent' of the deceiver emerged from the data as a meta-theme, whereby understanding an individual's motive and intent for engaging in deception will enable preparation for adversary deception to prevent vulnerabilities [19]. Differing intents to deceive whether to avoid being incarcerated for an act of criminality or to increase survival chances in a combat situation show a strong need to understand that deception occurs where there is intent. Past research has sought to uncover malign intent through questioning strategies [20]. However, it may be more pertinent to understand intent as part of a holistic approach to deception where the intent to deceive is regulated by adversary aims and motives and how situational elements will affect the timing of when deception occurs. This presents implications for how research into deception detection is conducted where participants are often automatically assigned to deception or truth-telling conditions excluding an individual's intent to deceive in specific contexts.

4.4. Deception Tactics

The third meta-theme of 'Deception Tactics' emerged from the dataset where the role of context is highlighted and different tactics for controlling information, influencing and deceiving the target are outlined. Sub-themes related to 'Deception Tactics' include: 'Context', 'Control of Information', 'Influencers', and 'Replicating Genuine Behavior'.

'Context' plays a large role in which tactic the deceiver will employ against the target, and how the situation, including communication channel, may change the form of interaction. Online communication has changed elements of the deception context, where there is a greater scale and reach of deceit and the potential for anonymity. In military deception it is argued that the same principles exist behind deception although contextual changes with the development of communication technologies have increased the range for deception. Previous research into deception has generally ignored the context of deception and how this impacts upon the target and whether cues to deception are generalizable across contexts. Research by [18] highlights understanding that people will behave according to the context they are in, this can further be expanded to how groups and organizations may seek to deceive others according to the situation. The holistic model of deception places a strong emphasis upon context and the situational factors that may lead to a deceiver choosing a specific tactic of deception.

'Control of Information' enables the deceiver to control what information is portrayed to the target. Through increasing the amount of information, the target receives, the deceiver can increase target ambiguity and cognitive load as there will be more information to process reducing the target's ability to respond to a situation. Through decreasing the amount of information, the target receives target ambiguity is also increased as the target will have less information with which to assess credibility. Deceivers often seek to control the way in which they present information whether verbal, non-verbal or physical to others and previous research has highlighted that deceivers may give shorter statements to their target to control their narrative and ensure consistency [25], but may also increase the number of individual details within their statement [34], potentially as a way of distracting the target from the deceptive content. Understanding how the deceiver may control information and the way in which they choose to release this information is required in detecting deception as this affects the strategy used to detect that deception.

'Influencers' highlights the various strategies that individuals use to persuade the target of their credibility. There are many techniques that can be used to influence others in everyday interactions, whether deception is occurring or not. Research examining persuasion tactics has identified key areas for influencing others [8] which has been applied to real-world activities, for example, advertising strategies. However, examining the impact of influence tactics in deception has been relatively neglected and the proposed model seeks to incorporate these.

One technique of appearing credible to others is through 'Replicating Genuine Behavior', whether the perception of genuine behavior is based upon lay beliefs or upon actual understanding of how to replicate behavior an awareness of both will be required to understand how differing individuals and adversaries will behave.

Replicating genuine behavior and appearance is a strategy that individuals seek to use in deceiving others

[24], however, this strategy may not always be effective as certain behaviors are harder to replicate in some contexts [39]. To date psychological research into exploring how deceivers replicate genuine behavior has mainly focused upon examples of deception in low-stakes environments where individuals may not have time to develop a plan for deception that often occurs in the strategic environment. Further understanding of the strategies that people use in high-stakes environments to appear genuine to others is required.

4.5. Interpretation

The fourth meta-theme of 'Interpretation' emerged from the dataset and lists the varying techniques and areas of focus which are used in deception detection across different communication mediums. Identified sub-themes for the 'Interpretation' enable an analysis of information: 'Source Attributes', 'Questioning/Interviewing Strategy', 'Detection Methods', 'Surveillance and ISTAR', and 'Risk'. The wide range of techniques uncovered for assessing veracity may also enable the development of bespoke strategies for detecting deception reflecting contexts in which deception occurs. 'Source Attributes' examines factors (consistency, plausibility, credibility and prominence) that enable a source, whether the source is an individual in a face-to-face setting or information in an online domain, to appear credible.

Past research in interpersonal deception has examined credibility as separate elements [49] rather than seeking to combine them enabling more accurate judgement about information. Research examining the credibility of websites has taken a more holistic approach to examining the source for credibility [13]. However, offering clear guidance on factors that enable analysis of sources across different communication channels as outlined above is required.

When interacting with potentially deceptive individuals in dyadic or triadic conversation 'Questioning/Interview Strategy' plays an important role in the generation of information to examine for deception or identify discrepancies for further examination, although as a factor it may not be applicable to all contexts. The cognitive interview may be used for questioning deceivers through discussing their statements extensively before requiring the deceiver to agree to their statement even if this contrasts with external evidence. Questioning and interviewing of individuals has often generated information for further analysis and has the potential for usage in conjunction with some verbal methods of detecting deception. Its inclusion in a holistic model to deception is required for usage in when we are interacting with individuals in interpersonal environments [9, 48].

Established techniques for examining information and intelligence for credibility emerged from the data set and 'Detection Methods' provide a range of techniques to detect deception from psychological and military backgrounds. Techniques to detect deception include verbal, non-verbal, pictorial, neuropsychological, paralinguistic and techniques used by military and intelligence personnel. These techniques will be utilized as part of a toolbox approach where the techniques used will fit the requirements of the situation. Previous research has begun to explore the use of multiple techniques to detect deception [4] and has found higher accuracy levels in detecting deception [39].

To uncover intelligence for assessment 'Surveillance and ISTAR' will enable the generation of information through varying surveillance techniques depending on the availability of channels for retrieving information and evidence. ISTAR techniques traditionally generate intelligence about an adversary which can then be used to inform decision-making, whilst approaches to deception detection have focused on identifying cues to deceit, though combining approaches verbal and non-verbal behavior can be analyzed alongside other intelligence, reflecting how deception is often detected in real-life [37].

In examining information for veracity there is always an element of 'Risk to Analyst' involved where incorrect decisions may have large consequences for organizations and an ability to examine risk is required. The impact of 'Risk to Analyst' on deception has been generally neglected within the deception literature with techniques focusing upon percentage of accuracy. However, in real-life situations relying upon probability may prove problematic, through adopting multiple approaches to deception detection adverse risk can be reduced.

4.6. Target

The final meta-theme of 'Target' emerged from the dataset which focuses upon the targets decision-making abilities and the factors that may affect the ability to accurately detect deception. Identified sub-themes that will affect the target are: 'Decision Making', 'Stakes', 'Individual Differences', 'Motivation', and 'Capabilities and Resources'. 'Decision Making' and how we make sense of the world is key to effectively detecting deception and mitigating risk. However, decision-making biases and attribution errors that the deceiver exploits may adversely affect the ability to detect deception. Decision-making biases have partially explained the

reasons for poor accuracy in detecting deceit, and an awareness of these biases and the decision-making process and their impact on the 'Interpretation' process is recommended to reduce error in detecting deception.

The 'Stakes' of a situation will affect the receiver and how they will judge a situation where potential deception may be occurring. The impact of stakes on the deceiver as this will affect their ability to appear credible and enhance the target's ability to more accurately detect deception. In everyday acts of deception, the deceit is often of little consequence and are used to maintain social harmony [5] therefore the target of that deceit may be less likely to question a situation. In cases related to strategic interests then stakes and the consequences of a decision will have a larger impact on the target and how risk is assessed.

A wide range of 'Individual Differences' affect our ability to accurately judge others including deception detection. Individuals with specific personality traits are better able to judge others personality, suggesting that individuals with such traits will best be placed to detect deception. Through understanding receiver individual differences [1] awareness of potential vulnerabilities and advantages emerges, and through understanding these vulnerabilities the risk of deception can be mitigated.

The target's 'Motivation' to detect deception will affect their ability to accurately detect deceit. Previous research has identified that motivated individuals are often less accurate in detecting deception [38], and this may occur where individuals rely upon lay strategies for detecting deception rather than cues identified by research. However, where individuals are motivated and have expertise in identifying genuine cues to deceit, motivation may have a reduced impact on decision-making errors.

Through understanding what 'Capabilities and Resources' are available the target will be able to ensure that they can recover information across varying communication channels, and they will have sources of expertise with which to analyze received information.

4.7. Limitations

The current research sought to validate and refine the holistic model of deception proposed by [41] by incorporating SME knowledge from a range of research and practitioner backgrounds. Volunteer bias suggests that this sample may not be representative of all SMEs in the field of deception and related areas and the specificity of the sample is acknowledged. Difficulties were encountered in accessing participants from security and intelligence backgrounds due to security reasons; therefore, it is acknowledged that there may be other techniques for detecting deception in military environments that the research has not incorporated into the holistic approach to deception. Further research may seek to address this issue through securing access to an SME sample with military and intelligence backgrounds.

4.8. Future Directions

The current research validates and refines the model of deception proposed by [41]; however, although strategies used to detect deception proposed by this model are outlined by SMEs there is a requirement for empirical validation. Future research should seek to examine the applicability of the model to real-world deception challenges, with a specific focus towards the online environment as an emerging area of risk. 'Red teaming' presents an option where rigorous analyses of the HMD can occur in a simulated real-world environment [10].

The 'Deceiver' meta-theme proposed by the current research states a strong requirement for cultural knowledge to understand an adversary and what may affect their attempts at deception and its detection. In addition, the focus on the mindset of individuals at any time when there is the need to identify future intent and incorporate an understanding of risk requires broader perspectives to be taken. Developing knowledge of these strategies may mitigate risk of deception. However, there is a current lack of research into cultural variations in how people deceive and seek to deceive others, specifically in the online environment, which presents additional challenges in an increasingly globalized world where individuals from differing cultural background interact daily, therefore future research should seek to address these concerns.

In assessing credibility there is always an element of risk involved in making decisions, especially in high-stakes environments where there may be large consequences for incorrect decisions. The current research has identified as sub-theme of 'Risk' in interpreting information that future research should examine in depth to acknowledge the element of risk involved in detecting deception and produce guidelines for reducing risk in high-stakes deceit.

An example of how deception may be identified and responded to may be developed from this model. If the deceiver had identified deception, cyber-deception through the range of identification tactics and strategies outlined in this mode. If the deceiver has been identified from their scent-trail or through mistakes in their website credibility or discourse, then the receiver can identify these mistakes and exploit them. They may then deploy the range of deception tactics and strategies outlined in this model. For example, if the deceiver has attempted to gain information through

phishing attacks, but has been identified then the target may send them false information in order to mislead them about their objectives.

5. Conclusion

In seeking to develop a holistic model of deception, the model proposed by [41] has been partially validated and refined through a series of interviews conducted with SMEs across the field of deception and influence. The current findings expand upon previous research into deception through formulating deception as a process whereby the deceiver conducts deception to achieve an aim motivated by their goals and affected by their culture, personality and mindset. The deceiver's choice of tactics and strategies with which to deceive will be reflective of context, communication channels and resources available to them, whilst the target has many techniques with which to interpret information and assess credibility, and the target in turn will be affected by individual differences, available resources and decision-making ability. In conclusion, it is argued that taking a more holistic perspective to viewing deception is required to mitigate risk.

10. References

[1] Aamodt, M. G., and H. Custer, H. "Who can best catch a liar? A meta-analysis of individual differences in detecting deception". The Forensic Examiner, 2006. 15: 6-11.

[2] Adams, S. H., and T. Harpster. "911 homicide calls and statement analysis". FBI Law Enforcement Bulletin. 2008, 77: 22-30.

[3] Bell, J. B. "Toward a theory of deception. International Journal of Intelligence and Counterintelligence", 2003. 16: 244-279. doi: 10.1080/08850600390198742.

[4] Bennett, M., and E. Waltz. Counterdeception Principles and Applications for National Security. Artech House: London. 2007.

[5] Bond, C. F., Jr., and B. M. DePaulo. "Accuracy of deception judgements". Personality and Social Psychology Review, 2006. 10: 214-234.

[6] Braun, V., and V. Clarke. "Using thematic analysis in psychology". Qualitative Research in Psychology, 2006. 3: 77-101. doi: 10.1191/1478088706qp063oa.

[7] Buller, D. B, and J. K. Burgoon. "Interpersonal deception theory". Communication Theory, 1996. 6: 203-242.

[8] Cialdini, R. B. Influence: The Psychology of Persuasion. New York: Harper Collins. 2007.

[9] Colwell, K., C., Hiscock-Anisman, C., and J. Fede. Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement. In B. S. Cooper, D. Griesel, and M. Ternes (Eds.). Applied Issues in Investigative Interviewing, Eyewitness Memory, and Credibility Assessment. (pp. 259-291). London: Springer. 2013.

[10] DCDC. Red Teaming Guide. Swindon: DCDC. 2013.

[11] DePaulo, B. M., S.E. Kirkendol, J. Tang, and T. P. O'Brien. "The motivational impairment effect in the communication of deception: replications and extensions". Journal of Nonverbal Behavior, 1988. 12: 177–202. doi:10.1007/BF00987487.

[12] Fogg, B. J. Prominence-Interpretation Theory: Explaining how people assess credibility. http://credibility.stanford.edu/pit.html. 2002.

[13] Fogg, B. J., C. Soohoo, D.R. Danielson, L. Marable, J. Stanford, and E. R. Tauber. "How do users evaluate the credibility of web sites? A study with over 2,500 participants". In Proceedings of the 2003 conference on designing for user experiences (DUX'03). http://portal.acm.org/citation.cfm?id=997097&coll=ACM&dl=ACM&CFID=36236037&CFTOKEN=18606069. 2003.

[14] Forster, P. K. "Countering individual jihad: Perspectives on Nidal Hasan and Colleen LaRose". Counterterrorism Exchange, 2012. 2: 1-11.

[15] George, J. F., K. Marett, and P. A. Tilley, P. A. "The effects of warnings, computer-based media, and probing activity on successful lie detection". IEEE Transactions on Professional Communication, 2008. 51: 1-17.

[16] Gerwehr, S. "Cross-cultural variation in denial and deception". Defense Intelligence Journal, 2006. 15: 51-78.

[17] Giordano, G., J. George, K. Marett and B. Keane. "Reviewers and the detection of deceptive information in recorded interviews". Journal of Applied Social Psychology, 2011. 41: 252-269.

[18] Gozna, L. F., and J. C. W. Boon. Interpersonal deception detection. In J.M. Brown and E.A. Campbell (Eds.). The Cambridge handbook of forensic psychology. (pp. 484-491). Cambridge: Cambridge University Press. 2010.

[19] Gozna, L. F., and R. Lawday. An applied scientist-practitioner model for the assessment of high-stake deceptive future intent in forensic and security settings: Incorporating critical consideration of personality, motive, mindset and risk. Poster presented at DECEPTICON 2015: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK. 2015.

[20] Granhag, P.A. and M. Knieps. "Episodic future thought: Illuminating the trademarks of forming true and false intentions". Applied Cognitive Psychology, 2011. 25: 274-280.

[21] Guest, G., K.M. MacQueen, and E. E. Namey. Applied Thematic Analysis. Los Angeles: Sage. 2012.

[22] Hancock, J. T., L. Curry, S. Goorha, S., and M. Woodworth. Automated linguistic analysis of deceptive and truthful synchronous computer-mediated communication. Paper presented at 38th Hawaii International Conference on System Sciences, Hawaii, USA. 2005.

[23] Hancock, J.T., M. Woodworth and S. Goorha, S. "See no evil: The effect of communication medium and motivation on deception detection". Group Decision and Negotiation, 2010. 19: 327-343.

[24] Hartwig, M., P. A. Granhag, L. A. Strömwall, and N. Doering. "Impression and information management: On the strategic self-regulation of innocent and guilty suspects". The Open Criminology Journal, 2010. 3: 10-16.

[25] Hartwig, M., P. A. Granhag and L.A. Strömwall, L. A. "Guilty and innocent suspects' strategies during police

interrogations". Psychology, Crime & Law, 2007. 13: 213-227.
[26] Heuer, R. J. Psychology of Intelligence Analysis. Washington, DC: U. S. Government Printing Office. 1999.
[27] Hilligoss, B., and S. Y. Rieh. "Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context". Information Processing and Management, 2008. 44: 1467-1484
[28] Hines, A., K. Colwell, C. Hiscock-Anisman, E. Garrett, R. Ansarra and L. Montalvo. "Impression management strategies of deceivers and honest reporters in an investigative interview". The European Journal of Psychology Applied to Legal Context, 2010. 2: 73-90.
[29] Jenkins, M. C., and C. J. Dando. Computer-mediated investigative interviews: A potential screening tool for the detection of insider threat. In S. Tomblin, N. MacLeod, R. Sousa-Silva, and M. Coulthard (Eds.). Proceedings of the 10th Biennial Conference of the International Conference of Forensic Linguistics, Birmingham: Center for Forensic Linguistics. 2012.
[30] Johnson, P. E., S. Grazioli, K. Jamal and I. A. Zualkernan. "Success and failure in expert reasoning". Journal of Organizational Behavior and Human Decision Processes, 1992. 53: 173-203.
[31] Kaina, J., M. G. Ceruti, K. Liu, S. C. McGirr, S. and J. B. Law. Deception detection in multicultural coalitions: Foundations for a cognitive model. Paper presented at the 16th International Command and Control Research and Technology Symposium (ICCTRS), Quebec, Canada. 2011.
[32] Mackay, A., and S. Tatham. Behavioural Conflict: Why Understanding People and Their Motivations Will Prove Decisive in Future Conflict. Saffron Walden: Military Studies Press. 2011.
[33] Metzger, M. J., and A. J. Flanagin. "Credibility and trust of information in online environments: The use of cognitive heuristics". Journal of Pragmatics, 2013. 59: 210-220.
[34] Morgan, C. A., K. Colwell and G. A. Hazlett. "Efficacy of forensic statement analysis in distinguishing truthful from deceptive eyewitness accounts of highly stressful events". Journal of Forensic Science, 2011. 56: 1227-1234.
[35] Newman, M. L., J. W. Pennebaker, D. S. Berry, and J. M. Richards, J. M. "Lying words: Predicting deception from linguistic styles". Personality and Social Psychology Bulletin, 2003. 29: 665-675.
[36] Ott, M., C. Cardie, and J. Hancock. Estimating the prevalence of deception in online review communities. Paper presented at WWW 2012, April 16–20, 2012, Lyon, France.
[37] Park, H. S., T. R. Levine, S. A. McCornack, K. Morrison and M. Ferrara, M. "How people really detect lies". Communication Monographs, 2002. 69: 144-157.
[38] Porter, S., S. McCabe, M. Woodworth, and K. A. Peace. "'Genius is 1% inspiration and 99% perspiration'… or is it? An investigation of the impact of motivation and feedback on deception detection". Legal and Criminological Psychology, 2007. 12: 297-309.
[39] Porter, S., and L. ten Brinke. "The truth about lies: What works in detecting high-stakes deception?" Legal and Criminological Psychology, 2010. 15: 57-75.
[40] Porter, S., L. ten Brinke, A. Baker and B. Wallace. "Would I lie to you? "leakage" in deceptive facial expressions relates to psychopathy and emotional intelligence". Personality and Individual Differences. 2011.
[41] Reid, I. D., L. F. Gozna, and J. C. W. Boon. Towards a holistic model of deception: The challenge of the cyber CHAMELEON. Poster presented at the 2nd MilDec Symposium, Defence Academy of the United Kingdom, Shrivenham, UK, 7-8 November. 2012.
[42] Sandham, A., T. Ormerod, C. Dando, R. Bull, M. Jackson, and J. Goulding. Scent trails: Countering terrorism through informed surveillance. Paper presented at Engineering Psychology and Cognitive Ergonomics – 9th International Conference, Orlando, Florida, USA. 2011.
[43] Stech, F. J., and C. Elsässer. Deception detection by analysis of competing hypotheses. Mclean, Virginia: The MITRE Corporation. 2003.
[44] Strömwall, L. A., and R. M. Willén. "Inside criminal minds: Offenders' strategies when lying". Journal of Investigative Psychology and Offender Profiling, 2011. 8: 271-281.
[45] Ten Brinke, L., and S. Porter. "Cry me a river: Identifying the behavioral consequences of extremely high-stakes interpersonal deception". Law and Human Behavior, 2012. 36: 469-477.
[46] Ten Brinke, L., S. Porter, and A. Baker. "Darwin the detective: Observable facial muscle contractions reveal emotional high-stakes lies". Evolution and Human Behavior. 2011
[47] Toma, C. L., J. T. Hancock, and N. B. Ellison. "Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles". Personality and Social Psychology Bulletin, 2008. 34: 1023-1036.
[48] Vrij, A. Detecting lies and deceit: The psychology of lying and the implications for professional practice. Chichester: Wiley. 2000.
[49] Vrij, A., L. Akehurst, S. Soukara, and R. Bull. "Detecting deceit via analysis of verbal and nonverbal behavior in children and adults". Human Communication Research, 2004: 30, 8-41.
[50] Vrij, A., H. Evans, L. Akehurst, and S. Mann. "Rapid judgements in assessing verbal and nonverbal cues: Their potential for deception researchers and lie detection". Applied Cognitive Psychology, 2004. 18: 283-296.
[51] Vrij, A., P. A. Granhag, S. Mann, and S. Leal. "Outsmarting the liars: Towards a cognitive lie detection approach". Current Directions in Psychological Science. 2011a. 20: 28-32.
[52] Vrij, A., P. A. Granhag, S. Mann, and S. Leal. "Lying about flying: The first experiment to detect false intent". Psychology, Crime & Law. 2011b. 17: 611-620.
[53] Warkentin, D., M. Woodworth, J. T. Hancock, and N. Cormier. Warrants and deception in computer mediated communication. Paper presented at CSCW, Savannah, Georgia, USA. 2010.
[54] Whaley, B. "Toward a general theory of deception". Journal of Strategic Studies, 1982. 5: 178-192.
[55] Whaley, B., and J. Busby. Detecting deception: Practice, practitioners, and theory. In R. Godson & J. J. Wirtz. (Eds.). Strategic Denial and Deception: The Twenty-First Century Challenge. (pp. 181-221). London: Transaction Publishers. 2002.

2020-01-07

Toward a holistic model of deception: subject matter expert validation

Reid, Iain D.

University of Hawaii at Manoa

Reid ID, Black R. (2020) Toward a holistic model of deception: subject matter expert validation.
In: 53rd Hawaii International Conference on System Sciences, 7-10 January 2020, Maui, Hawaii
https://doi.org/10.24251/HICSS.2020.230